UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/656,074	09/06/2000	Elliott Glazer	10655.9200	9142

20322 7590 05/04/2005

SNELL & WILMER
ONE ARIZONA CENTER
400 EAST VAN BUREN
PHOENIX, AZ 850040001

EXAMINER	
NALVEN, ANDREW L	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 05/04/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/656,074	GLAZER ET AL.	
	Examiner	Art Unit	
	Andrew L. Nalven	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 February 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☒ Claim(s) *25-28* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *2/14/05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-28 are pending.

Response to Arguments

2. Applicant's arguments filed 22 February 2005 have been fully considered but they are not persuasive.

3. Applicant has argued on pages 6-7 that the Matias reference fails to teach "upon retrieving the data, formatting the retrieved data in real-time at said server, wherein the formatted data includes at least one authenticity key." Examiner respectfully disagrees. Examiner initially notes that the feature of the "authenticity key" has been cited to the Atkinson reference and thus arguments alleging Matias' lack of teaching of this feature are spurious. Examiner has relied upon Matias to teach the real-time formatting of retrieved data. Examiner contends that Matias teaches upon retrieving the data, formatting the retrieved data in real-time at said server (Matias, column 7 lines 29-43) by teaching the retrieving of data Dc,v (Matias, column 7 lines 29-35) and the formatting of the data into a response message (Matias, column 7 lines 28-40) by applying a key K in a message authentication procedure. Thus, while Examiner has not relied upon Matias to teach the authenticity key, Examiner does contend that Matias teaches an authenticity key included in a formatted message. Examiner maintains the previous rejection and contends that Atkinson also teaches an authenticity key included in

retrieved data by teaching a hash value included in a file that is used to assure authenticity of a received file (Atkinson, column 5 line 64 – column 6 line 28).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-3, 8-9, 13-16, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Atkinson et al US Patent No 5,892,904 in view of Matias et al US Patent No 6,681,017. Atkinson discloses a system for code certification of network transmissions.

6. With regards to claims 1 and 14, Atkinson teaches receiving a data request from a client (Atkinson, column 1 lines 19-48), retrieving data based on the received data request (Atkinson, column 1 lines 19-48, column 5 lines 37-44), formatting the retrieved data wherein the formatted data includes at least one authenticity key (Atkinson, column 5 line 64 – column 6 line 28), returning the formatted data to the client (Atkinson, column 6 lines 11-16), and authenticating the authenticity key to verify the source of the formatted data (Atkinson, column 6 lines 8-9 and 44-49). Atkinson fails to teach the formatting occurring in real time at the server. Matias teaches that upon retrieving the data, formatting of the retrieved data occurs in real time at the server (Matias, column 7

lines 29-43, mac and nonce). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Matias' method of applying formatting in real time with Atkinson's code certification system because it offers the advantage of providing the client a simple method of verifying that a server response is associated with a client request (Matias, column 2 lines 35-48).

7. With regards to claims 2 and 15, Atkinson as modified teaches the formatted data being a web page (Matias, column 4 lines 1-9, web page).

8. With regards to claims 3 and 16, Atkinson as modified teaches the reading of the formatted data at the client (Atkinson, column 7 lines 35-38), determining if the formatted data includes the at least one authenticity key (Atkinson, column 7 lines 35-45), and verifying authenticity based on the authenticity key if it is included (Atkinson, column 7 lines 27-30).

9. With regards to claims 8 and 13, Atkinson teaches a client, server, and a network wherein the client and server communicate (Atkinson, Figure 2A), an authentication server that is in communication with the server (Atkinson, column 5 line 64 – column 6 line 16), and an authentication server being configured to insert an authenticity key into the data requested from the client thereby facilitating the client to authenticate the authenticity key to verify the source of the data (Atkinson, column 6 lines 1-17), but fails to teach the data requested being a webpage. Matias teaches the data requested being a webpage (Matias, column 4 lines 1-9, web page). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Matias' method of applying formatting in real time to a web page with Atkinson's code

certification system because it offers the advantage of providing the client a simple method of verifying that a server response is associated with a client request (Matias, column 2 lines 35-48).

10. With regards to claim 9, Atkinson as modified teaches a client including a browser (Atkinson, column 5 lines 47-44) wherein pages are displayed to a user on a display device on the client (Atkinson, column 5 lines 45-63).

11. With regards to claim 20, Atkinson as modified teaches the receiving and returning steps being implemented via at least one of the Internet, interactive television system, broadband system, regular band system, wireless system, radio transmission, landline phone system, and cellular phone system (Atkinson, column 5 lines 25-35).

12. Claims 4, 6, 10-11, 17, and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Atkinson et al US Patent No 5,892,904 in view of Matias et al US Patent No. 6,681,017, as applied to claims 3, 8, 10 and 16 above, and in further view of Wallent et al US Patent No 6,366,912.

13. With regards to claims 4 and 17, Atkinson as modified teaches the verification of an authenticity stamp (Atkinson, column 7 lines 23-30) but fails to teach the displaying of the data based on the verification of the authenticity key. Wallent discloses a browser that displays data based on the verification of a security rules (Wallent, column 11 line 18 – column 12 line 3). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Wallent's method of displaying data after verifying the security procedures because it offers the advantage of allowing

the browsing of the World Wide Web while reducing the risks of malicious code being downloaded from a web page (Wallent, column 1 lines 24-37 and column 2 lines 10-19).

14. With regards to claims 6 and 23, Atkinson as modified teaches an authenticity key being applied to each file (Atkinson, column 6 lines 11-16) but fails to teach the file being a graphic file. Wallent teaches the downloading to a user of a web page as described above and the web page including a graphic file (Wallent, column 1 lines 31-35).

15. With regards to claims 10-11, Atkinson as modified teaches the adding of an authentication key to an object and its subsequent verification but fails to specifically teach the object being a page and thus a server sending a page to the client. Wallent teaches a server sending a page to a client (Wallent, Figure 9). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Wallent's method of applying security to web pages sent from a server because it offers the advantage of allowing the browsing of the World Wide Web while reducing the risks of malicious code being downloaded from a web page (Wallent, column 1 lines 24-37 and column 2 lines 10-19).

16. Claims 5, 7, 12, and 18-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Atkinson et al US Patent No 5,892,904, of Matias et al US Patent No. 6,681,017 and Wallent et al US Patent No 6,366,912 as applied to claims 4, 11, and 17 above, and further in view of Houser et al US Patent No 5,606,609.

17. With regards to claims 5 and 18, Atkinson as modified above fails to teach the displaying of an authenticity stamp. Houser teaches an authenticity stamp being displayed for data that has been successfully verified (Houser, column 8 lines 12-15 and column 7 lines 52-59). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Houser's method of displaying an authenticity stamp because it offers the advantage of providing a user friendly deterrent to forgery and alterations to documents (Houser, column 3 lines 15-46).

18. With regards to claim 7 and 19, Atkinson as modified above fails to teach the displaying of a non-authenticity stamp. Houser teaches an non-authenticity stamp being displayed for data that has been unsuccessfully verified (Houser, column 16 lines 44-48).

19. With regards to claim 12, Atkinson as modified above fails to teach the display including an indication of the authenticity based on the authenticity key. Houser teaches an authenticity stamp being displayed when an authenticity stamp is verified (Houser, column 8 lines 12-15 and column 7 lines 52-59). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Houser's method of displaying an authenticity stamp because it offers the advantage of providing a user friendly deterrent to forgery and alterations to documents (Houser, column 3 lines 15-46).

20. Claim 21 is rejected under 35 U.S.C. 103(a) as being unpatentable over Atkinson et al US Patent No 5,892,904 in view of of Matias et al US Patent No. 6,681,017, as

applied to claim 1 above, and in further view of Asad et al US Patent No 6,539,093. Asad discloses a key ring organizer for an electronic business using public key infrastructure.

21. With regards to claim 21, Atkinson as modified teaches the step of authenticating the authenticity key to verify the source of the formatted data (Atkinson, column 6 lines 8-9 and 44-49), but fails to teach the use of a browser plug-in interfacing with a MIME type. Asad teaches the use of a browser plug-in interfacing with a MIME type (Asad, column 7 lines 22-35). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Asad's method of using plug-ins interfacing with a MIME type with Atkinson as modified because it offers the advantage of allowing the certification of third party keys by way of a browser initiating a request message to the plug-in (Asad, column 3 lines 20-42).

22. Claim 22 is rejected under 35 U.S.C. 103(a) as being unpatentable over Atkinson et al US Patent No 5,892,904 in view of Matias et al US Patent No. 6,681,017, as applied to claim 8 above, and in further view of Walker et al US Patent No 6,286,001. Walker discloses a system and method for authorizing access to data on content servers in a distributed network.

23. With regards to claim 22, Atkinson as modified fails to teach the authentication server verifying a user ID and password. Walker teaches the authentication server verifying a user ID and password (Walker, column 11 lines 45-53). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to

utilize Walker's user ID/password method with Atkinson as modified because it offers the advantage of allowing greater control over the authorization to view designated web sites (Walker, column 2 lines 52-64).

24. Claim 24 is rejected under 35 U.S.C. 103(a) as being unpatentable over Atkinson et al US Patent No 5,892,904 in view of Matias et al US Patent No. 6,681,017 and in further view of Kou US Patent No 6,016,491. Kou discloses a generic file format for multiple security requirements.

25. With regards to claim 24, with regards to claims 1 and 14, Atkinson teaches receiving a data request from a client (Atkinson, column 1 lines 19-48), retrieving data based on the received data request (Atkinson, column 1 lines 19-48, column 5 lines 37-44), formatting the retrieved data wherein the formatted data includes at least one authenticity key (Atkinson, column 5 line 64 – column 6 line 16), returning the formatted data to the client (Atkinson, column 6 lines 11-16), and authenticating the authenticity key to verify the source of the formatted data (Atkinson, column 6 lines 8-9 and 44-49). Atkinson fails to teach the formatting occurring in real time at the server and the determining if the data includes a code that requires the data to be authenticated. Matias teaches that upon retrieving the data, formatting of the retrieved data occurs in real time at the server (Matias, column 7 lines 29-43, mac and nonce). Kou teaches the determining if the data includes a code that requires the data to be authenticated (Kou, column 5 lines 9-28). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Matias' method of applying formatting in

real time and Kou's method of determining if security is needed with Atkinson's code certification system because it offers the advantage of providing the client a simple method of verifying that a server response is associated with a client request (Matias, column 2 lines 35-48) and providing flexibility because different pieces of information require different forms of security protection (Kou, column 1 lines 31-35).

26.

Allowable Subject Matter

27. Claims 25-28 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

28. The following is a statement of reasons for the indication of allowable subject matter: The prior art fails to teach the decrypting of a preferences key, the decrypting of a preference file using the preferences key, obtaining instructions within the preferences file, and inserting a visual signature into said data based on the instructions stored in the preferences file, as defined in the limitations of the cited claims and thus fails to anticipate or render the above limitations obvious.

Conclusion

29. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Andrew L. Nalven whose telephone number is 571 272 3839. The examiner can normally be reached on Monday - Thursday 8-6, Alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on 571 272 3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Nalven
ALN

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100